

**UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH CAROLINA
COLUMBIA DIVISION**

Richard G. Beck and Lakreshia R. Jeffery,)
on behalf of themselves and all)
others similarly situated)

Plaintiffs,)

vs.)

Eric K. Shinseki, in his Official Capacity as)
Secretary of Veterans Affairs,)

Rebecca Wiley, Medical Director of)
William Jennings Bryan Dorn VA Medical)
Center,)

Barbara Temeck, M.D., Chief of Staff of)
William Jennings Bryan Dorn VA Medical)
Center,)

Ruth Mustard, RN, Director for Patient)
Care/Nursing Services of William Jennings)
Bryan Dorn VA Medical Center,)

David L. Omura, Associate Director of)
William Jennings Bryan Dorn VA Medical)
Center, and)

Jon Zivony, Assistant Director of William)
Jennings Bryan Dorn VA Medical Center,)

Defendants.)

Civil Action No.:

COMPLAINT

(Jury Trial Demanded)

(Class Action)

COME NOW PLAINTIFFS, Richard G. Beck and William H. Prince on behalf of
themselves and all others similarly situated, would respectfully show unto the court as follows:

NATURE OF THE ACTION

1. This is an action for declaratory and injunctive relief and money damages for Defendants' violations of federal law, including but not limited to, the Administrative Procedure Act ("APA"), the Privacy Act ("Privacy Act"), and the Health Insurance Portability and Accountability Act ("HIPAA"), each as amended. Plaintiffs seek to represent approximately 7,500 individuals who have suffered emotional trauma, monetary damages, and been placed in fear of identity theft, destruction of credit, and health insurance fraud because of Defendants' willful and intentional actions and reckless disregard for the privacy of these citizens' personal identifying and medical information (the "Class").

2. On or about February 11, 2013, Defendants suffered the loss or theft of a laptop computer containing the private personal and medical information of approximately 7,500 veterans who had received medical treatment in Defendants' facilities in this state, specifically the William Jennings Bryan Dorn VA Medical Center ("Dorn VAMC").

3. The private personal and medical information ("Personal Information") on the lost or stolen laptop computer was not encrypted or otherwise safeguarded by Defendants as required by law, policy, minimum accepted standards, and Defendants' repeated public representations.

4. Defendants failed to properly perform the duties and responsibilities of their respective positions within the Department of Veterans Affairs by failing to require compliance with applicable federal regulations, policies, and procedures regarding Privacy Act and HIPAA records and did not ensure that Plaintiffs' privacy rights were protected from the intentional, willful, reckless, arbitrary, and capricious actions and inactions of other Defendants and their agents, servants, and employees.

5. Defendants flagrantly disregarded the privacy rights of affected veterans, including Plaintiffs, by illegally, intentionally, and willfully ignoring, and knowingly allowing its employees, contractors, servants, and other Department officials to ignore the requirements of

Department rules, other federal regulations, applicable policies and procedures for creating, maintaining, accessing, disclosing, and using Personal Information contrary to law.

6. Defendants' intentional, willful and reckless disregard for Plaintiffs' privacy rights are most obvious in their failing to make even the most rudimentary effort to safeguard Plaintiffs' Personal Information from unauthorized disclosure and theft despite nearly seven years to implement the lessons from a notorious 2006 event involving the loss of the private personal information of more than 26 million veterans and several subsequent similar events. Thus, Plaintiffs' Personal Information was unencrypted, easily copied, physically accessible, and left available to anyone obtaining physical control of the laptop. Defendants' failure to implement competent safeguards, or to base any safeguards on a reasonable and up-to-date security threat analysis, allowed Plaintiffs' Personal Information to literally walk out the door.

7. Defendants' intentional, willful and reckless actions and inactions have inflicted, and will long continue to inflict, real costs and emotional pain and suffering on Plaintiffs.

JURISDICTION AND VENUE

8. Jurisdiction of this Court is invoked pursuant to 28 U.S.C. § 1331 because this is a civil action arising under the laws of the United States. Jurisdiction is also invoked pursuant to 5 U.S.C. §§ 552a(g)(1), (5) because this is a civil action to enforce a liability created under 5 U.S.C. § 552a after September 27, 1975.

9. Venue is appropriate in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the claims occurred in this district.

PARTIES

10. Plaintiff Richard Beck is a citizen and resident of Richland County, South Carolina, and is an honorably discharged veteran who has received pulmonary and cardiovascular treatment or other health care at Dorn VAMC.

11. Plaintiff Lakreshia R. Jeffery is a citizen and resident of Richland County, South

Carolina, and is an honorably discharged veteran who received pulmonary and cardiovascular treatment or other health care at Dorn VAMC.

12. Defendant Eric K. Shinseki is the Secretary of Veterans Affairs and is the official responsible for the proper execution and administration of all laws administered by the Department of Veterans Affairs.

13. Defendant Rebecca Wiley is the VAMC Medical Director and, among other duties, is an official responsible for the proper execution and administration of the laws relevant to operation of the facility.

14. Defendant Barbara Temek, M.D., is the Dorn VAMC Chief of Staff and, among other duties, is an official responsible for the proper execution and administration of the laws relevant to operation of the facility.

15. Defendant Ruth Mustard, RN, is the Dorn VAMC Director for Patient Care/Nursing Services and is responsible for the proper execution among other duties, is an official responsible for the proper execution and administration of the laws relevant to operation of the facility.

16. Defendant David L. Omura is the Dorn VAMC Associate Director of the William Jennings Dorn VA Medical Center and, among other duties, is an official responsible for the proper execution and administration of the laws relevant to operation of the facility.

17. Defendant Jon Zivony is the Dorn VAMC Assistant Director of the William Jennings Dorn VA Medical Center, and, among other duties, is an official responsible for the proper execution and administration of the laws relevant to operation of the facility.

18. The parties to this action and the acts and omissions complained of herein are subject to the jurisdiction of this court.

STATEMENT OF THE FACTS

19. On or about February 11, 2013, a laptop computer was reported missing from a testing laboratory in the Dorn VAMC Respiratory Therapy Department. The laptop computer and hard drive admittedly contained private personal and medical information, including information subject to the Privacy Act and HIPPA pertaining to approximately 7,500 United States military veterans (the “Personal Information”). The missing laptop and its embedded Personal Information included individual identifying information including, but not limited to, names, addresses, phone numbers, social security numbers, and dates of birth. In addition, an unknown number of records contained veterans’ confidential medical and disability information. Upon information and belief, the laptop computer was not stored in a security container and none of the Personal Information was encrypted or similarly protected.

20. To date the subject laptop computer has not been returned to Defendants and it, and the Personal Information contained in it, remains unaccounted for.

21. Upon information and belief, Plaintiffs’ Personal Information was improperly gathered and placed on the missing laptop computer by an employee(s), agent(s), contractor(s), or other servant(s) of the Department of Veterans Affairs and the Personal Information was retrieved or retrievable by the name of each individual or by some identifying number, symbol, or other identifying particular assigned to an individual.

APA VIOLATIONS

22. As of at least February 11, 2013, Defendants were required, at a minimum, to comply with the “Privacy Act Guidelines – July 1, 1975” published in the Federal Register on July 9, 1975, unless the requirements therein were subsequently modified or eliminated. In addition, Defendants were required to comply with numerous federal statutes, regulations, technical standards, as well as Department policies and procedures promulgated since the Department’s 2006 loss of a laptop containing the personal information of 26 million veterans.

23. Well before February 11, 2013, Department regulations, e.g., 38 C.F.R. § 1.576, and numerous Department policies and Directives required Defendants to safeguard an individual against an invasion of privacy, to collect, maintain, use, or disseminate records of personally identifiable information in a manner that assures that such action is for a necessary and lawful purpose, and to ensure that adequate safeguards are provided to prevent misuse of such information.

24. Well before February 11, 2013, other federal rules, regulations, procedures and guidance documents established minimum standards for Defendants' actions in gathering, maintaining, disclosing, using, and safeguarding personal and medical information, including, Office of Management and Budget guidelines, Federal Information Processing Standards, National Institute of Standards and Technology ("NIST") standards.

25. On or about February 11, 2013, Defendants failed to comply, and failed to ensure compliance, with the applicable laws and standards or have adequate and appropriate policies and procedures in place to prevent the loss of Plaintiffs' Personal.

26. Defendants' failures are especially egregious in light of the repeatedly acknowledged safeguard failures, including a security breach at another VA medical facility in 2007 under essentially indistinguishable circumstances, and widely disseminated reports of the lack of management concern with implementing adequate safeguards.

UNAUTHORIZED DISCLOSURE

27. The Privacy Act requires that personal information maintained by government agencies, including Defendants, only be disclosed (1) upon written authorization of the individual to whom the information pertains or (2) to persons who have been authorized to access the information pursuant to applicable regulations and procedures and then only for specified "routine" uses.

28. Plaintiffs did not give Defendants written permission for their Privacy Act Records and other Personal Information to be placed on the laptop that was stolen from Defendants' facility.

29. The use of Plaintiffs' Personal Information was not authorized pursuant to Defendants' administrative requirements, in that there was no submission of a formal request for access and a formal authorization granting access had not been executed.

30. Defendants' failure to physically safeguard Plaintiffs' Personal Information is further evidenced in that the individual or individuals that took and retain physical control of the missing laptop containing Plaintiffs' Personal Information was not challenged by Defendants, or any other VA employees, regarding his or her authority to possess, access, or use the subject laptop computer and remain unknown and at large.

FAILURE TO SAFEGUARD

31. Minimum requirements and standards for federal information security have long been available to federal agencies and officials, and the Department and Defendants are well aware of their responsibilities and duties under those requirements. Further, the Department has made almost innumerable commitments to veterans, Congress, and the American people that it would properly safeguard personal information after 2006 when it lost control of the personal information of an estimated 26 million veterans and their families. Among the most repeated commitments was that Department laptop computers potentially containing personal information would be encrypted to prevent unauthorized access should the device be lost or stolen.

32. Defendants have not met their commitments and have again failed to protect veterans personal information, including Plaintiffs' Personal Information. Defendants' failures are all the more egregious in this case because they were aware of ongoing gaps in security, including a 2007 loss of a laptop improperly containing personal information from a Birmingham VA medical facility under essentially the same circumstances as in this case.

33. Well before February 11, 2013, Defendants were, or should have been, aware of inherent and obvious risks associated with the removal of data from a protected environment that could result in potential disclosure of Personal Information through loss or theft. Indeed, the theft of a VA laptop computer is an all too frequent occurrence, and the Defendants have long been on notice of the risks of such an event, yet still failed to ensure that proper safeguards were in place to prevent such an occurrence at Dorn VAMC.

34. In addition, Defendants have been grossly negligent, if not willfully blind, in encrypting devices containing personal information. VA's own Office of Inspector General reported only a few months before the February 13, 2013, incident that, although Defendants spent \$3,700,000.00 in 2006 to purchase encryption software, they had installed that software on only 16% of the devices for which it was purchased. In other words, nearly seven years after committing to encrypt personal information on Department computers, at least 335,000 devices remain unprotected. Further, the VA OIG stated unequivocally that the cause of this incredibly poor performance was Defendants' "inadequate planning and management."

35. It is also clear that Defendants remain without an adequate physical security process and has not implemented any means to identify unauthorized personnel in secure areas containing laptop computers or prevent the removal of the stolen equipment from VA workplaces.

FAILURE TO PUBLISH NOTICE

36. The Privacy Act and implementing regulations require Defendants to publish notice of the creation of any new system of records and the purpose for such system in the Federal Register.

37. Contrary to these requirements, Defendants did not issue any such notice regarding the system of records maintained on the missing laptop and it was not reasonably possible for any individual whose Personal Information was included in the system of records

created on the laptop to determine that their individually identifying information was contained in that system of records or otherwise maintained by VA outside of a properly noticed system of records.

INTENTIONAL AND WILLFUL VIOLATIONS

38. One or more of Defendants' employees, agents, contractors, or servants intentionally and willfully transferred Plaintiffs' Personal Information to the missing laptop and stored the information outside of the applicable administrative requirements and without appropriate safeguards.

39. Numerous federal laws, including 44 U.S.C. § 3534, require that Defendants implement information security for information systems that support VA operations which include: (1) periodic assessments of the risk and magnitude of harm that could result from the unauthorized access and use of that information; and (2) policies and procedures that are based on those risk assessments. Defendants did not require or ensure compliance with these fundamental information security requirements.

40. Long-standing weaknesses in Defendants' information security systems were responsible for the February 11, 2013, data breach. Defendants failed to heed years of warnings about lax security from its own Inspector General and other agencies such as the Government Accountability Office, and failed to implement numerous and repeated recommendations for correction.

41. Defendants knew, or should have known, that their officers, employees, contractors, agents, or servants had ignored or failed to enforce VA and other federal requirements for ensuring that Personal Information, including Privacy Act and HIPPA records were accessible only by properly authorized individuals, but did not require compliance therewith.

42. High level VA officials intentionally and willfully ignored specific and repeatedly identified weaknesses and vulnerabilities regarding improper laptop use. Any competent security professional or organization charged with safeguarding sensitive information, such as Privacy Act and HIPPA records, would categorize storing files on a computer system without any hardware or software security barriers as a fundamental security threat. Indeed, Defendants have been repeatedly warned of these fundamental deficiencies by security professionals.

43. Defendants' inaction towards the persistent, unabating, and unaddressed security threats presented by the unmonitored activities of their employees, agents, contractors, and servants constitutes intentional and willful conduct so reckless as to exceed the standard of conduct for gross negligence.

44. Further exacerbating the harm from their inactions, once Defendants lost control of Plaintiffs' Personal Information, Defendants failed to timely report the event to Plaintiffs. Upon information and belief, Defendants waited well over a month before notifying anyone outside the Department of the safeguards failure, without good cause for that delay.

ADVERSE EFFECTS AND DAMAGES

45. Each of Defendants' failures complained of caused Plaintiffs adverse impacts and harm including, but not limited to, embarrassment, inconvenience, unfairness, mental distress, and the threat of current and future substantial harm from identity theft and other misuse of their Personal Information. The threat of identity theft, medical insurance abuse, and similar adverse effects caused by Defendants' violations requires continuing affirmative actions by Plaintiffs to recover peace of mind, emotional stability, and personal security including, but not limited to, frequently obtaining and reviewing credit reports, bank statements, health insurance reports, and other similar information, obtaining credit watch services, and closing financial accounts.

46. Plaintiffs have, and will continue to, suffer tangible and intangible harm as a result of Defendants' failures and violations for the foreseeable future. This harm includes pecuniary and non-pecuniary damages.

CLASS ACTION ALLEGATIONS

47. This action is maintainable as a class action pursuant to Federal Rules of Civil Procedure 23(a), (b)(1)-(3).

48. The class consists of all persons who have been adversely effected by Defendants' violations of law and failure to safeguard Plaintiffs' Personal Information.

49. The class is so numerous that joinder of all members is impracticable. The class size is approximately 7,500, which is the number of individuals whose information Defendants admit was collected and maintained on the missing laptop.

50. Joinder of class members' individual actions is impractical because of the geographical diversity of class members, the limited ability of individual class members to institute separate suits, and the general nature of the underlying action and relief sought.

51. Class representatives' counsel is appropriately qualified and experienced to represent the class.

52. There are substantial questions of fact and law common to all class members. The legal issues raised in this Complaint include violations of the APA, Privacy Act, HIPAA, and state law causes of action. The factual issues of whether Defendants violated one or more legal requirements are common to all class members. The facts, circumstances, and merits of the case, therefore, apply equally to all class members.

53. The claims of the representative Plaintiffs are typical of the claims of the class members. Representative Plaintiffs are military veterans who reasonably believe that their personal information was improperly safeguarded and improperly disclosed by Defendants.

54. The representative Plaintiffs will fairly and adequately protect the interests of the class. Furthermore, the representative Plaintiffs' claims span the breadth of issues raised in this action.

55. The prosecution of separate actions by individual class members would create a risk of inconsistent results that could establish incompatible standards of conduct for Defendants.

56. Defendants' liability for damages can be established by facts and circumstances common to the class as a whole and do not require the examination of Plaintiffs' individual circumstances.

57. Questions of law and fact common to members of the class predominate over any questions affecting only individual members.

58. A class action is superior in this case to other methods for a fair and efficient adjudication of the controversy because: (A) the common interests of the class members predominate over any individual interest in controlling prosecution or control of separate actions; (B) no similar litigation concerning the controversy is known to have been commenced by members of the class; (C) concentrating litigation of this action in this Court is appropriate to ensure appropriate, consistent, and efficient resolution of the constitutional issues raised in the district where the offending conduct occurred, continues to occur, and could occur in the future; and (D) the difficulties in managing an action involving this class are significantly reduced by existing databases of potential class members prepared by the government and veteran service organizations.

FIRST CLAIM FOR RELIEF

Violations of the Administrative Procedure Act

59. Plaintiffs reassert their allegations set forth above and incorporate them by reference into this First Claim for Relief.

60. On February 11, 2013, a number of federal rules, regulations, procedures, and standards governed Defendants' actions in gathering, maintaining, disclosing, using, and safeguarding Privacy Act records and systems of records and information protected under HIPPA. Each of the applicable federal rules, regulations, procedures and standards were final actions of a promulgating federal agency.

61. Defendants were ultimately responsible for control, direction, and management of VA's processes, policies, and procedures for compliance with all applicable federal rules, regulations, procedures and standards.

62. Defendants intentionally, willfully and unlawfully withheld and unreasonably delayed, required action, or acted so recklessly as to exceed the standard of conduct for gross negligence with respect to the applicable federal rules, regulations, procedures and standards for implementing the Privacy Act and HIPAA. Defendants' actions in this regard were also arbitrary, capricious and an abuse of discretion and were taken without observance of procedure required by law.

63. Plaintiffs were adversely affected and aggrieved as a result of Defendants' improper actions and inactions and are entitled to equitable relief for Defendants' violation of Plaintiffs' rights pursuant to the APA, 5 U.S.C. §§ 702, 704, and 706 and the inherent equitable powers of the Court.

SECOND CLAIM FOR RELIEF

Violation of the Privacy Act – Unauthorized Disclosure

64. Plaintiffs reassert their allegations set forth above and incorporate them by reference into this Second Claim for Relief.

65. Defendants were responsible for ensuring that only individuals authorized pursuant to approved rules, regulations, procedures and standards compliant with the Privacy Act could access Plaintiffs' Privacy Act records.

66. Defendants failed to ensure that only VA employees, contractors, agents, and servants who had submitted access authorization requests, completed background checks, and met each of the other authorization process requirements could access VA Privacy Act systems of records. Upon information and belief, Defendants also failed to maintain any records of granted authorizations, requested or completed background checks, or to ensure that the sensitivity level that employees, agents, contractors and/or servants seeking to access Privacy Act records matched the sensitivity level of the information to be accessed. Defendants' failures allowed an individual unauthorized use and access to and use of Plaintiffs' Privacy Act records contained on the subject laptop computer for unauthorized and improper purposes.

67. Defendants flagrantly disregarded Plaintiffs' privacy rights and caused Plaintiffs adverse effects by disclosing Plaintiffs' Privacy Act records to unauthorized persons, in violation of 5 U.S.C. § 552a(b).

68. Defendants' violation of the Privacy Act disclosure requirements were intentional or willful, or was the result of conduct so reckless as to exceed the standard of conduct for gross negligence.

69. Defendants' intentional and willful Privacy Act violations caused Plaintiffs to suffer actual damages and Plaintiffs are entitled to monetary damages and the costs of this action together with reasonable attorney fees pursuant to the Privacy Act and 5 U.S.C. § 552a(g).

THIRD CLAIM FOR RELIEF

Violation of the Privacy Act – Failure to Safeguard

70. Plaintiffs reassert their allegations set forth above and incorporate them by reference into this Third Claim for Relief.

71. Defendants flagrantly disregarded Plaintiffs' privacy and caused Plaintiffs adverse effects by failing to establish and ensure lawful compliance with appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to

protect against anticipated threats or hazards to the records security or integrity, which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information was maintained, in violation of 5 U.S.C. §§ 552a(e)(9), (10).

72. Defendants' violation of the Privacy Act safeguards requirements and to prevent or mitigate the effects of unauthorized and unmonitored employee transfer of sensitive data, including Privacy Act records, was either intentional and willful or the result of professional incompetence so reckless as to exceed the standard of conduct for gross negligence.

73. Defendants' intentional and willful Privacy Act violations caused Plaintiffs to suffer actual damages and Plaintiffs are entitled to monetary damages and the costs of this action together with reasonable attorney fees pursuant to the Privacy Act and 5 U.S.C. § 552a(g).

FOURTH CLAIM FOR RELIEF

Violation of the Privacy Act – Improper Purpose

74. Plaintiffs reassert their allegations set forth above and incorporate them by reference into this Fourth Claim for Relief.

75. There is not, and never has been, any statute or executive order of the President authorizing Defendants to establish a system of records for the purpose for which the Personal Information on the missing laptop was reportedly used or for existing VA Privacy Act records or system of records to be used for that purpose.

76. Defendants flagrantly disregarded Plaintiffs' privacy and caused Plaintiffs adverse effects by assembling and maintaining Plaintiffs' Personal Information in a system of records although the information was not relevant and necessary to accomplish a purpose required by statute or by executive order of the President in violation of 5 U.S.C. § 552a (e)(1).

77. Defendants' violation of the Privacy Act proper purpose requirement was intentional and willful or the result of conduct so reckless as to exceed the standard of conduct for gross negligence.

78. Defendants' Privacy Act violations caused Plaintiffs to suffer actual damages and Plaintiffs are entitled to monetary damages and the costs of this action together with reasonable attorney fees pursuant to the Privacy Act and 5 U.S.C. § 552a(g)

FIFTH CLAIM FOR RELIEF

Violation of the Privacy Act – Failure to Publish Notice

79. Plaintiffs reassert their allegations set forth above and incorporate them by reference into this Fifth Claim for Relief.

80. Defendants are responsible under the Privacy Act for ensuring that individuals whose personal information is maintained by VA are informed of, *inter alia*, the fact that the government is maintaining the information, the location of the information, the purpose for maintaining the information, the authority to gather and maintain the information, and the safeguards used to protect the information from improper disclosure or abuse.

81. Defendants failed to publish a Federal Register notice pursuant to 5 U.S.C. § 552a(e)(4) informing Plaintiffs that a new system of records was created, being maintained, the purpose for maintaining the information, the safeguards being implemented, or the authority to gather and maintain the information.

82. Defendants further failed to ensure that Plaintiffs were informed of the maintenance of their personal information in the that system of records through an accurate Federal Register notice in violation of 5 U.S.C. § 552a(e)(4).

83. Defendants flagrantly disregarded Plaintiffs' privacy by failing to publish a notice in the Federal Register of the system of records maintained on the missing laptop.

84. Defendants' violation of the Privacy Act notice requirement was intentional and willful or the result of conduct so reckless as to exceed the standard of conduct for gross negligence.

85. Defendants' Privacy Act violations caused Plaintiffs to suffer actual damages and Plaintiffs are entitled to monetary damages and the costs of this action together with reasonable attorney fees pursuant to the Privacy Act and 5 U.S.C. § 552a(g).

SIXTH CLAIM FOR RELIEF

NEGLIGENCE PER SE

86. Plaintiffs reassert their allegations set forth above and incorporate them by reference into this Sixth Claim for Relief.

87. Defendants owed a duty to Plaintiffs to properly secure the subject laptop computer containing Plaintiffs' personal information in violation of statutory law including the APA, the Privacy Act, HIPAA and Federal Regulations.

88. The HIPAA Security Rule, 45 C.F.R. § 164.306 requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting electronic protected health information (ePHI). Specifically, covered entities must:

- a. Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
- b. Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- c. Protect against reasonably anticipated, impermissible uses or disclosures; and
- d. Ensure compliance by their workforce.

89. Defendants were also required by HIPAA to review and modify their security measures to continue protecting e-PHI, to analyze their own needs and implement solutions to maintain safeguards against the dissemination of Plaintiffs' ePHI.

90. Defendants failed to inform the Plaintiffs of the theft of the subject laptop and the breach of security of Plaintiffs' medical records and personal information in a prompt and timely

manner thus further exposing the Plaintiffs to pecuniary and non-pecuniary damages including but not limited to identity theft, fraud loss of peace of mind, emotional instability, pecuniary loss associated with obtaining credit watch services, emotional distress and out-of-pocket costs.

91. Defendants owed a duty to Plaintiffs to comply with statutory law by properly securing their medical records and personal information which were contained on the stolen subject laptop.

92. As a direct and proximate result of Defendants' gross negligence per se, recklessness, willfulness, and wantonness, Plaintiffs have suffered actual damages and are in imminent danger of suffering further material injury and loss by being placed in a material risk of harm for identity theft.

93. As a result of the above described gross negligence per se, recklessness, willfulness, and wantonness, Plaintiffs are entitled to a judgment against Defendants for actual damages, statutory damages, attorneys' fees, incidental damages, and costs in the amount to be determined by the trier of fact.

SEVENTH CLAIM FOR RELIEF

SOUTH CAROLINA COMMON LAW NEGLIGENCE

94. Plaintiffs reassert their allegations set forth above and incorporate them by reference into this Seventh Claim for Relief.

95. Defendants failed to properly secure the subject laptop computer containing Plaintiffs' personal information in violation of numerous statutes and regulations.

96. Defendants failed to inform the Plaintiffs of the breach of security in their medical records and personal information in a prompt matter further exposing the Plaintiffs to damages including but not limited to pecuniary and non-pecuniary damages including but not limited to

identity theft, fraud loss of peace of mind, emotional instability, pecuniary loss associated with obtaining credit watch services, emotional distress and out-of-pocket costs.

97. Defendants owed a duty to Plaintiffs to comply with statutory law and federal regulations by properly securing their medical records and personal information which were contained on the stolen subject laptop.

98. Defendants have failed to exercise slight care or the care necessary under the circumstances and have willfully, recklessly, wantonly and with gross negligence violated and failed to comply with the duties imposed upon them, through statutory and regulatory mandates to secure Plaintiffs' personal information, and report any such breach of privacy in the most expedited manner possible

99. Defendants have willfully, wantonly, recklessly, and with gross negligence violated and failed to comply with the duties imposed upon them, through statutory and regulatory mandates to secure Plaintiffs' personal information, and report any such breach of privacy in the most expedited manner possible.

100. As a direct and proximate result of Defendants' gross negligence, recklessness, willfulness, and/or wantonness, Plaintiffs have suffered actual damages and are in imminent danger of suffering further material injury and loss by being placed in a material risk of harm for identity theft.

101. As a result of the above described gross negligence, recklessness, willfulness, and/or wantonness, Plaintiffs are entitled to a judgment against Defendants for actual damages, incidental damages, attorneys fees, statutory damages and costs in the amount to be determined by the trier of fact.

EIGHTH CLAIM FOR RELIEF
SOUTH CAROLINA COMMON LAW
NEGLIGENT HIRING, TRAINING, SUPERVISION AND RETENTION

102. Plaintiffs reassert their allegations set forth above and incorporate them by reference into this Eighth Claim for Relief.

103. Plaintiffs are informed and believe that Defendants were negligent, careless, reckless, wanton, willful and grossly negligent at the time and place hereinabove mentioned in the following particulars:

- a. In failing to have in place policies and procedures to properly hire, train, retain, supervise and monitor its employees, agents, contractors and/or servants, or if such procedures were in place, in failing to enforce them;
- b. In failing to have in place adequate policies and procedures to mandate compliance by its employees, agents, contractors and/or servants with statutes, laws, regulations and standards of care related to the security of Plaintiffs' and veterans' personal information and Privacy Records, or if such policies and procedures were in place, in failing to enforce them;
- c. In generally failing to use the degree of care and caution required under the same or similar circumstances; and
- d. In such others as may be ascertained through discovery in this matter.

104. That because of the acts and/or omissions of Defendants as enumerated hereinabove which resulted both proximately and directly in the damages also set out above, the Plaintiffs seek a reasonable amount of actual damages against the Defendants as well as an exemplary amount of punitive damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray as follows:

- (a) That this Court issue a declaratory judgment that Defendants violated, and continue to violate, Plaintiffs' rights under the Administrative Procedure

Act, Privacy Act of 1974, and the Health Insurance Portability and Accountability Act

- (b) That this Court enjoin Defendants and the officers, agents, contractors, employees, and servants of the Department of Veterans Affairs, and those acting for and with them, to account for all the Privacy Act and HIPPA records in the Department's Columbia Regional Office and Dorn Medical Center possession or under control, including all copies, whether authorized or unauthorized, on agency and personal computers, and on any data storage medium and to cause to be recovered or permanently destroyed any records or personal information derived from those records that is found in any unauthorized or improper location or maintained contrary to consensus industry or federal standards for information security and safeguards, the Court to retain jurisdiction until such accounting is favorably reviewed by a panel of acknowledged experts in information security independent of Defendants and approved by the Court;
- (c) That this Court enjoin Defendants and the officers, agents, contractors, employees, and servants of the Department of Veterans Affairs, and those acting for and with them from transferring agency Privacy Act or HIPPA records or any information compilation derived or based on Privacy Act or HIPPA records from agency computer systems to any portable device capable of storing, containing, or transferring any record or system of records, including, but not limited to, laptop computers, CDs, DVDs,

portable hard drives, memory sticks or similar devices, and “iPods” and similar devices, from property under Defendants’ supervision and control until and unless Defendants demonstrate to the Court that adequate information security has been established pursuant to the applicable federal standards;

- (d) That this Court grant to Plaintiffs judgment against Defendants for damages in an amount allowed by statute for each individual who suffered damages resulting from Defendants’ intentional and willful Privacy Act violations, such amount to exceed \$100,000.00;
- (e) That this Court grant to Plaintiffs their costs and reasonable experts’ and attorney’s fees;
- (f) For an order certifying the class defined herein, appointing undersigned counsel as class counsel, approving Plaintiffs as class representative, and requiring that notice be provided to the class.
- (g) That this Court grant such additional relief as the Court deems proper and just.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray as follows:

- (a) That this Court issue a declaratory judgment that Defendants violated, and continue to violate, Plaintiffs’ rights under the Administrative Procedure Act, Privacy Act of 1974, and the Health Insurance Portability and Accountability Act;
- (b) That this Court enjoin Defendants and the officers, agents, contractors,

employees, and servants of the Department of Veterans Affairs, and those acting for and with them, to account for all Privacy Act and HIPPA records in the possession of the Department's Columbia Regional Office and Dorn Medical Center or under their control, including all copies, whether authorized or unauthorized, on agency and personal computers, and on any data storage medium and to cause to be recovered or permanently destroyed any records or personal information derived from those records that is found in any unauthorized or improper location or maintained contrary to applicable standards for information security and safeguards, the Court to retain jurisdiction until such accounting is favorably reviewed by a panel of acknowledged experts in information security independent of Defendants and approved by the Court;

- (c) That this Court enjoin Defendants and the officers, agents, contractors, employees, and servants of the Department of Veterans Affairs, and those acting for and with them from transferring agency Privacy Act or HIPPA records or any information compilation derived or based on Privacy Act or HIPPA records from Department computer systems to any portable device capable of storing, containing, or transferring any record or system of records, including, but not limited to, laptop computers, CDs, DVDs, portable hard drives, memory sticks or similar devices, and "iPods" and similar devices, from property under Defendants' supervision and control until and unless Defendants demonstrate to the Court that adequate information security has been established pursuant to the applicable

federal standards;

- (d) That this Court grant to Plaintiffs judgment against Defendants for damages in an amount calculated to compensate each individual who suffered damages resulting from Defendants' violations, actions, and inactions;
- (e) That this Court grant to Plaintiffs judgment against Defendants for punitive damages to the degree allowed by law in an amount calculated to deter Defendants from continuing to ignore their duties and responsibilities to safeguard the private personal and medical information entrusted to them;
- (f) That this Court grant to Plaintiffs their costs and reasonable experts' and attorney's fees;
- (g) For an order certifying the class defined herein, appointing undersigned counsel as class counsel, approving Plaintiffs as class representatives, and requiring that notice be provided to the class; and
- (h) That this Court grant such additional relief as the Court deems proper and just.

Respectfully Submitted,

MIKE KELLY LAW GROUP, LLC

BY: /s/ D. Michael Kelly
D. Michael Kelly
Fed. Id. No. 2299
Brad D. Hewett
Fed. Id. No. 10388
Walton J. McLeod, IV
Fed. Id. No. 10549
500 Taylor Street

P.O. Box 8113
Columbia, SC 29202
803/726-0123

/s/ Douglas J. Rosinski
Douglas J. Rosinski, Esq.
Fed. Id. 6995
701 Gervais St., Ste. 150-405
Columbia, SC 29201-3066
803.256.9555 (tel)
888.492.3636 (fax)
djr@djrosinski.com

Attorneys for Plaintiffs

Columbia, South Carolina
April 12, 2013